IN THE CLAIMS

A presentation of all of the pending claims with their current status indicated follows.

1. (Canceled)

2. (Previously presented) The method as defined in claim 11, wherein the sequence number is transmitted together with the signing key from the control center to the sender, and is transmitted from the sender via the data set to the receiver.

3. (Previously presented) The method as defined in claim 11, wherein the sequence numbers are used to produce signing keys in the control center and corresponding checking keys in the receiver.

4. (Previously presented) The method as defined in claim 11, wherein the sequence numbers are used to produce signing keys used in the control center and corresponding check keys are used in the receiver wherein the sequence number is transmitted via the data set to the receiver.

5. (Previously presented) The method as defined in claim 11, wherein the sequence number is produced by a pseudo-random number generator.

6. (Previously presented) The method as defined in claim 11, wherein the encryption of the sequence number by means of the main key is used as the one-time encryption.

7. (Currently Amended) The method as defined in claim 11, wherein the control center produces a number of pairs of signing keys and sequence numbers, and transmits [[~~them~~]] the signing keys to the sender, either separately or together as pairs with the associated sequence numbers.

8. (Previously presented) The method as defined in claim 11, wherein the receiver maintains a list of already used sequence numbers, and rejects already used sequence numbers.

9. (Currently Amended) A device for signing a message which is sent from a sender to a receiver comprising:

a control center having a first memory and a receiver having a second memory each storing [[~~for~~]] a secret, common main key;

the control center including, one input of a first one-time encrypter being connected to the first memory of the control center, and another input being connected to a generator for a sequence number,

an output of the first one-time encrypter being connected to the sender via a transport medium;

a signature generator provided in the sender, and having inputs connected to the output of the first one-time encrypter and to the message to be signed;

an output of the signature generator providing a signature and being connected to a device which assembles at least the signature and the message to form a data message block and whose output is connected to the receiver via a transport medium;

a signature checker provided in the receiver having inputs connected to the message and to the signature of the data message block which has arrived via the transport medium, and wherein

the inputs of the signature checker are further connected to an output of a second one-time encrypter for providing a check key, whose inputs are connected to the second memory of the receiver for the secret main key and to a means for [[~~providing~~]] determining a sequence number for the received data message block, the check key and the determined sequence number being used to form a calculated signature for comparison to the signature of the data message block.

10. (Previously presented) The device as defined in claim 9, wherein the generator to produce a sequence number uses a deterministic method to produce one or more sequence numbers that correspond to the same number of check keys.

11. (Currently Amended) A method for signing a message from a sender and for checking a signature at a receiver, the method comprising the steps of:

[[~~initializing~~]] storing, in a control center [[,]] and a receiver, [[~~with~~]] a shared main key;

causing the control center to produce one or more sequence numbers;

using a selected one of the sequence numbers and the shared main key to create a signing key by means of a one-time encryption;

providing at least one pair of the signing key and the selected sequence number to the sender via a secure transmission;

the sender using the at least one pair of the signing key and the selected sequence number to form a signature for a message;

the sender forming a data set;

the sender sending the message to the receiver via the data set containing at least the message and the signature;

determining, at the receiver, [[~~the~~]] a sequence number [[~~from~~]] for the received data set;

passing the determined sequence number and the shared main key through a one-time encryption to produce a check key; [[~~and~~]]

using the check key and the determined sequence number to form a calculated signature; and

comparing the calculated signature to the received signature to verify the [[~~signature~~]] received message.

Please add the following new claims.

-- 12. (New) The method as defined in claim 2, wherein the selected sequence number is transmitted via the data set from the sender to the receiver, the step of determining a sequence number includes extracting the sequence number from the received data set.

13. (New) The method as defined in claim 5, the step of determining a sequence number includes:

storing, at the receiver, an initial value for the pseudo-random number generator; and

when a data set is received at the receiver, producing a new value of the sequence number.

14. (New) The method as defined in claim 11, wherein the sequence numbers are comprised of one of decreasing numbers, numbers with a step interval greater than unity and numbers representing a date and time, the time including a number of seconds from an appointed start time.

15. (New) The method as defined in claim 11, wherein the secure transmission of the signing key and the selected sequence number between the control center and the sender includes one of printing on security paper and storage in a smart card.

16. (New) The method as defined in claim 11, wherein the calculated signature and the received signature are the same when the check key and the signing key are the same.

17. (New) The method as defined in claim 11, wherein the control center is comprised of a control center for a financial institution, the sender is comprised of one of a manufacturer of an automated cash dispensing mechanism and a local branch of the financial institution, and the receiver is comprised of an automatic cash dispensing mechanism. --